Amendments to the Drawings:

The attached drawing sheet includes changes to Figure 3. In Figure 3, labels "&" of adders (171) and (181) have been removed.

REMARKS/ARGUMENTS

In the Office Action mailed November 4, 2008, claims 1-19 were rejected. Additionally, the drawings were objected to. In response, claims 1, 5, and 13 have been amended and claims 15-19 have been canceled. Additionally, claims 20-25 have been added. The drawings have also been amended. Applicant hereby requests reconsideration of the application in view of the amended claim, the new claims, and the below-provided remarks.

For reference, support for claim 20 is found in Applicant's specification at, for example, Fig. 1 and original claims 13 and 15. Support for claim 21 is found in Applicant's specification at, for example, Fig. 1 and original claims 13 and 16. Support for claim 22 is found in Applicant's specification at, for example, Fig. 1 and original claims 13 and 17. Support for claim 23 is found in Applicant's specification at, for example, original claims 8 and 13. Support for claim 24 is found in Applicant's specification at, for example, original claims 9 and 13. Support for claim 25 is found in Applicant's specification at, for example, original claims 10 and 13.

Objections to the Drawings

The drawings were objected to because adders (171) and (181) of Figure 3 were incorrectly labeled with "&." In response, the labels "&" of the adders (171) and (181) of Figure 3 have been removed. Thus, Applicant respectfully requests that the objections to the drawings be withdrawn.

Claim Rejections under 35 U.S.C. 101

Claims 1-12, 18, and 19 were rejected under 35 U.S.C. 101 as being directed to non-statutory subject matter. In particular, the Office Action states that the claims are directed to a method or process for performing a multiplication via a mathematical algorithm to produce a multiplication result. The Office Action further states that the claims are not limited to a practical application of the mathematical algorithm because the multiplication is not a tangible result.

Claims 18 and 19 have been canceled and therefore the rejections to claims 18 and 19 under 35 U.S.C. 101 are moot.

Claim 1 has been amended to recite a method "for implementing a cryptographic algorithm in an electronic device" that includes "using the final result to complete an encryption or decryption operation within the electronic device." Support for the amendments to claim 1 is found in Applicant's specification at, for example, page 1, lines 8-10 and page 1, lines 15-18, respectively. Applicant respectfully submits that claims 1-12 are directed to statutory subject matter because these claims recite a process, which places them squarely within the categories defined by 35 U.S.C. 101 (i.e., processes, machines, manufactures, and compositions of matter). In particular, the preamble of amended claim 1 recites "A method for implementing a cryptographic algorithm in an electronic device that includes performing modular multiplication of integers X and Y to produce a result R, where R=X.Y mod N, in a multiplication engine."

The MPEP states that the tangible requirement requires that the claim must recite more than a 35 U.S.C. 101 judicial exception (i.e., abstract idea, mathematical algorithm, natural phenomenon, or law of nature). MPEP 2106(IV)(C)(2)(2)(b). Where a claim includes a reference to subject matter included in the judicial exceptions, the process claim must set forth a practical application of that judicial exception to produce a real-world result. The MPEP also states that the tangible requirement does not necessarily mean that a claim must either be tied to a particular machine or apparatus or must operate to change articles or materials to a different state or thing. Here, the method limitations of claims 1-12 are tied to structural components of a machine or apparatus. In particular, amended claim 1 recites an electronic device. Claims 2-12 depend from and include all of the limitations of claim 1 and, hence, include the indirect reference to the indicated physical structures.

Additionally, the specification explains that the method operations of claims 1-12 have a practical application of implementing a cryptographic algorithm in an electronic device and completing an encryption or decryption operation within the electronic device. In other words, at least one practical application of the claimed method is to implement a cryptographic algorithm in an electronic device and to complete an encryption or decryption operation within the electronic device. Since the recited method claims are

tied to physical structures and the specification explains a practical application of the method, Applicant respectfully submits that claims 1-12 satisfy the requirements set forth in the MPEP with respect to determining whether a claimed invention complies with 35 U.S.C. 101. Accordingly, Applicant requests that the rejection of claim 1-12 under 35 U.S.C. 101 be withdrawn.

Claim Rejections under 35 U.S.C. 102

Claims 15-17 were rejected under 35 U.S.C. 102(b) as being anticipated by Shah et al. (U.S. Pat. Pub. No. 4,864,529, hereinafter "Shah"). Claims 15-17 have been canceled and therefore the rejections under 35 U.S.C. 102 are moot.

Claim Rejections under 35 U.S.C. 112

Claims 1-19 were rejected under 35 U.S.C. 112, second paragraph, as allegedly being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. In particular, claims 1 and 13 were rejected because the phrase "pre-calculated multiples" appears to be mis-descriptive. Additionally, claim 1 was rejected because the term "so" does not follow from the proceeding language. Claim 15 was rejected because the term "each" should be deleted and because of some grammatical errors. Claims 15-19 have been canceled, thereby rendering the rejections to claims 15-19 moot. Claims 1 and 13 have been amended to replace the phrase "pre-calculated multiples" with the term "products." Support for the amendments to claims 1 and 13 is found in Applicant's specification at, for example, page 5, lines 21-24. Additionally, claims 1 and 13 have been amended to replace the phrase "so as to" with the term "to." The amendments that have been made address the above-identified defects. Thus, Applicant respectfully requests that the claim rejections under 35 U.S.C. 112 be withdrawn.

Claims 1-14

Claims 1-12 were rejected under 35 U.S.C. 112 and under 35 U.S.C. 101. As described above, claim 1 has been amended to overcome the rejections under 35 U.S.C.

112 and under 35 U.S.C. 101. Thus, Applicant respectfully asserts that amended claim 1 is now in the condition for allowance.

Claim 5 has been amended to correct a previous mistake. In particular, claim 5 has been amended to replace the item "$(x_{n-j+1}y_2 + r_{j-1,1})B_y$" with the item "$(x_{n-j+1}y_2 + r_{j-1,1})B_y^2$." Claim 2-12 depend from and incorporate all of the limitations of the independent claim 1. Therefore, Applicant respectfully asserts that claims 2-12 are allowable at least based on an allowable claim 1.

Claim 13 has been further amended to remove a reference number, to replace a comma with a period, and to add a term "the method." Claim 13 was rejected only under 35 U.S.C. 112. As described above, claim 13 has been amended to overcome the rejection under 35 U.S.C. 112. Thus, Applicant respectfully asserts that amended claim 13 is now in the condition for allowance.

Claim 14 depends from and incorporates all of the limitations of the independent claim 13. Therefore, Applicant respectfully asserts that claim 14 is allowable at least based on an allowable claim 13.

New Claims 20-25

New claim 20 is similar to original claim 15. Claim 15 was rejected under 35 U.S.C. 112, second paragraph, because of the term "each" and because of some grammatical errors. Applicant respectfully submits that new claim 20 does not include the above-identified term "each" or the noted grammatical errors.

New claims 23-25 are similar to original claims 8-10, respectively, which are method claims. Claims 8-10 were rejected under 35 U.S.C. 101 as allegedly being directed to non-statutory subject matter. Applicant respectfully submits that claims 23-25 are directed to statutory subject matter because claims 23-25 recite an apparatus, which places them squarely within the categories defined by 35 U.S.C. 101 (i.e., processes, machines, manufactures, and compositions of matter). In particular, claims 23-25 are directed to the "Apparatus for performing modular multiplication of integers," as recited in claim 13.

Claims 20-25 depend from and incorporate all of the limitations of the independent claim 13. Applicant respectfully asserts that claims 20-25 are allowable at least based on an allowable claim 13.

CONCLUSION

Applicant respectfully requests reconsideration of the claims in view of the amendments and remarks made herein. A notice of allowance is earnestly solicited.

Respectfully submitted,

/mark a. wilson/

Date: February 4, 2009

Mark A. Wilson
Reg. No. 43,994

Wilson & Ham
PMB: 348
2530 Berryessa Road
San Jose, CA 95132
Phone: (925) 249-1300
Fax: (925) 249-0111